REMARKS

Entry of this Amendment is proper because it does not raise any new issues requiring further search by the Examiner, narrows the issues on appeal, and is believed to place the present application in condition for immediate allowance.

Claims 1-3 and 5-36 are all the claims presently pending in the application.

While Applicants' believe that the claims are patentable over the cited references, to speed prosecution, Applicants amend independent claims 1, 24, 31, and 33 to define more clearly the features of the invention.

It is noted that the claim amendments are made only for more particularly pointing out the invention, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicants specifically state that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1-3 and 5-36 stand rejected on prior art grounds. Claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Borza (U.S. Patent No. 6,446,210). Claims 5-8 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza. Claims 10-13, 19, 21-23, 29, and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza and further in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon").

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention relates to a method of processing semiotic data.

In an illustrative, non-limiting aspect of the invention, as defined, for example, by independent claim 1, a method of processing semiotic data includes receiving semiotic data including a data set P, selecting a function h, and for at least one of each the data set P to be collected, computing h(P), destroying the data set P, storing h(P) in a database, and to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' is close to some P, wherein the data set P cannot be extracted from h(P).

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

II. THE PRIOR ART REJECTIONS

A. Claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36 stand rejected under 35 U.S.C. §102(e) as being anticipated by Borza.

For the Examiner's convenience, the traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004 are incorporated herein by reference in their entirety.

In the "*Response to Arguments*" of the present Office Action, the Examiner states that Applicants' arguments have been fully considered but they are not persuasive (see Office Action at page 2, numbered paragraph 4).

The Examiner also asserts that, in response to Applicant's argument that the references fail to show certain features of eh invention, the features upon which Applicants rely (i.e., how such a comparison [comparing the encrypted data against an encrypted template] could be implemented or accomplished) allegedly are not recited in the rejected claims (see Office Action at page 2, numbered paragraph 5).

The Examiner further states that, with regard to Applicants' arguments that Borza fails to disclose means-plus-function language, the Examiner respectfully disagrees. In the comments made with regards to the interview conducted 04 August 2004, the Applicants point out in particular that Borza fails to discuss claim 27 recitation of "means for encrypting each said at least one data set acquired to form at least one encrypted data set," the examiner points to Figure 3, specifically blocks 53, to show that Borza does indeed disclose means for encrypting. This is further discussed in at least column 5, lines 34-47. With regards to the rest of the means-plus-function language, the Examiner could not find where the means for performing the various functions are discussed in the specification and has therefore given the claims their broadest reasonable interpretation. The Examiner further states that '[t]his rejection can be overcome by pointing to where in the Specification that the means language exists and if the means taught in the Specification differs from the teachings of Borza (see Office Action at pages 2-3, numbered paragraph 7).

While Applicants' believe that the claims are patentable over the cited references, <u>to speed prosecution</u>, Applicants amend independent claims 1, 24, 31, and 33 to define more clearly the features of the invention.

Accordingly, Applicants respectfully submit that there are elements of the claimed invention which clearly are <u>not</u> disclosed or suggested by Borza. Therefore, Applicants respectfully traverse this rejection.

Applicants respectfully submit that Borza does <u>not</u> disclose or suggest how to compare encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template, according to the present invention.

For example, independent claim 1 recites a method of processing semiotic data, comprising:

> selecting a function h, and for at least one of each said data set P to be collected, computing h(P);
> <u>destroying said data set P;</u>
> storing h(P) in a database, and
> <u>to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' is close to some P,</u>
> wherein said data set P cannot be extracted from h(P)
> (emphasis added).

That is, the claimed invention is not determining whether h(P) matches h(P'), as allegedly disclosed by Borza. Instead, the claimed invention is determining whether P is close to P' by comparing only h(P) with h(P'). Borza does not disclose or suggest this feature of the claimed invention, or for that matter, even contemplate the problem solved by the claimed invention.

Applicants submit that Borza does not disclose or suggest comparing encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data).

In comparison, the present invention is adapted to accommodate the lack of absolute reproducibility in the observation of personal data. The present invention discloses that, in the application of DNA typing, there exist two kinds of personal data with regard to reproducibility: (1) those data with absolute reproducibility, which are based on based on Polymerase Chain Reaction (PCR) methods, and (2) those data which, because of measurement uncertainty, add a degree of irreproducibility in the matching process (see specification at page 15, lines 1-7).

The present invention describes that it is necessary to devise ways to protect personal data when it is not perfectly reproducible. This irreproducibility means that the data set does not determine perfectly its reading (see specification at page 16, lines 4-7). For example, because P0 is in general (possibly) slightly different from Pi for i>0, the secret version of P0 will generally be quite different from the secret version of Pi. Thus, no identification is possible by direct comparison of the encrypted data (see specification at page 16, lines 12-17).

Indeed, the present invention discloses three methods that can be used to circumvent this situation and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19).

In comparison, Applicants respectfully reiterate that, while Borza generally describes comparing the encrypted data against an encrypted template (see Borza at column 8, lines 28-38), Borza simply mentions this only a single time in the disclosure and does not elaborate on this feature again. That is, Borza does not disclose or suggest with sufficient specificity how such a comparison could be implemented or accomplished.

Indeed, Applicants respectfully reiterate that the method described by Borza could not work in general, since such a comparison would generally be based on comparing matching scores and, because encryption diffuses the data, such comparison against the scores of encrypted data would not work (e.g., without significantly altering the accuracy and sensitivity of the identification process).

Specifically, a new data P' is matched against data P in the database if P' is "close" to P. However, the diffusive nature of encryption would ensure that h(P) would be far from h(P').

Thus, Applicants respectfully reiterate that it would not be possible to match h(P) against h(P'), according to the disclosure of Borza.

On the other hand, the claimed invention provides specific solutions to this problem (e.g., see specification at pages 17-20) and defined by novel and unobvious combination of elements recited in claims 1-3 and 5-36.

Accordingly, Applicants respectfully submit that Borza neither discloses nor suggests at least "to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' is close to some P", in as complete detail as recited, for example, in independent claim 1.

Thus, for the foregoing reasons, Applicants respectfully submit that Borza does not disclose or suggest all of the features of claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36.

Therefore, the Examiner respectfully is requested to reconsider and withdraw this rejection and to permit these claims to pass to immediate allowance.

B. Claims 5-8 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza.

Applicants respectfully submit that claims 5-8 are patentable over Borza for somewhat similar reasons as those set forth above with respect to independent claim 1.

Moreover, with respect to claim 5, the Examiner acknowledged that Borza does not disclose or suggest destroying the private key K and sending the private key K to a trusted party. However, the Examiner alleged that if would have been obvious to destroy the private key K and send the private key to a trusted third party, since it allegedly is known in the art that the private key is needed to decrypt any message encrypted with the public key k, and therefore, the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k.

Applicants respectfully reiterate that, assuming *arguendo* that it is known in the art that the private key is needed to decrypt any message encrypted with the public key k and that the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k, it would not have been obvious to modify Borza to arrive at the claimed combination of features recited in the claimed invention.

For example, Borza merely relates to a method for enhancing network security for a communication session initiated between a first computer and a second computer (e.g., see Borza at Abstract).

On the other hand, the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, <u>without significantly altering the accuracy and sensitivity of the identification process</u> (e.g., see specification at page 3, lines 9-14).

As described in an illustrative embodiment of the invention, for each **P** to be collected, h(P) is computed, P is destroyed, and h(P) is stored in a database (e.g., see specification at page 14, lines 10-11). In the claimed invention, the private key K is maintained, if at all, only by a trusted third party (e.g., the Supreme Court, the FBI, etc.) and P cannot be extracted from h(P) except by the trusted party (e.g., see specification at page 14, lines 7-15). Otherwise, h(P') is compared to all available h(P)s to determine if one of them matches, as recited, for example, in claim 7.

Thus, Applicants respectfully reiterate that Borza does not disclose or suggest all of the features of claims 5-8, and further, that it would not have been obvious to modify Borza to arrive at the claimed combination of features recited in the claimed invention.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw this rejection of claims 5-8.

C. Claims 10-13, 19, 21-23, 29, and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza and further in view of Kharon.

Applicants respectfully submit that claims 10-13, 19, 21-23, 29, and 35 are patentable over Borza for somewhat similar reasons as those set forth above with respect to, for example, independent claim 1.

On the other hand, Applicants respectfully reiterate that Kharon does not make up for the deficiencies of Borza, and therefore, independent claims 1, 9, 19, 29, or 35 would not have been obvious over Borza or Kharon, either alone or in combination. Indeed, the Examiner does not even rely on Kharon for the disclosure of such features, as mentioned above.

Moreover, Applicants respectfully reiterate that claims 10-13, 19, 21-23, 29, and 35 also are patentable over Borza or Kharon, either alone or in combination, by virtue of the additional, novel and unobvious combination of features recited therein.

For example, with respect to claim 10 (see Office Action, numbered paragraph 23), while Kharon appears to describe how minutia in fingerprints are compared, Kharon does not describe the claimed method of computing subcollections and encrypting them (see Kharon at column 13, lines 43-67).

In comparison, a novel and unobvious aspect of the claimed invention is not merely to use a smaller data set, but to use many smaller subsets of the original data set and encrypting such smaller subsets of the original data set.

As with Borza, in Kharon, unencrypted minutiae data must be compared, since the encryption would diffuse the data, and therefore, would render comparison against a threshold impossible (e.g., see Kharon at column 14, lines 28-39, and column 15, lines 42-55).

As another example, with respect to claims 12 and 23 (e.g., see Office Action, numbered paragraph 26), while Borza appears to describe the possibility of false rejection, Borza does not teach or suggest that the computation of the variations is possible with a particular piece of biometric data (e.g., see Borza at column 11, lines 25-34).

Similarly, Borza also does not teach or suggest the computation of variations (e.g., see Borza at column 12, lines 25-61).

Further, while Borza appears to describe encrypting the data before transmission, Borza does not describe comparing encrypted data against encrypted data in the database (e.g., see Borza at column 12, lines 25-61).

Also, while Borza appears to describe how multiple biometric data can be used to authenticate a person, Borza does not address how to compare encrypted data. (e.g., see Borza at column 11, line 65 to column 12 line 34).

Thus, for the foregoing reasons, Applicant respectfully reiterate that neither Borza nor Kharon discloses or suggests all of the features of claims 10-13, 19, 21-23, 29, and 35.

Therefore, the Examiner respectfully is requested to reconsider and withdraw this rejection of claims 10-13, 19, 21-23, 29, and 35.

III. CONCLUSION

In view of the foregoing, Applicants submit that claims 1-3 and 5-36, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: January 18, 2005

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (703) 872-9306 the enclosed Amendment under 37 C.F.R. § 1.116 to Examiner Christian A. La Forgia on January 18, 2005.

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386